

# SOPHOS

## Sophos Control Center Guide de démarrage

Version du produit : 4.1

Date du document : février 2011



## Table des matières

1 À propos de ce guide.....	3
2 Configuration requise.....	4
3 Installation.....	5
4 Protection des ordinateurs en réseau.....	9
5 Vérification de la protection des ordinateurs.....	12
6 Paramétrage des alertes par courriel.....	13
7 Paramétrage de la recherche des applications potentiellement indésirables.....	15
8 Traitement des virus.....	17
9 Configuration du pare-feu.....	18
10 Support technique.....	21
11 Copyright.....	22

## 1 À propos de ce guide

Ce guide vous indique comment protéger vos ordinateurs en réseau (ordinateurs Windows et Mac) contre les virus (y compris les spywares), les applications potentiellement indésirables et toutes les autres menaces de sécurité.

Si vous avez des ordinateurs qui ne sont jamais connectés à votre réseau, reportez-vous également au *Guide de démarrage pour postes autonomes de Sophos Endpoint Security and Control*.

Si vous procédez à la mise à niveau depuis une version antérieure de Sophos Control Center, reportez-vous au *Guide de mise à niveau de Sophos Control Center*.

Pour plus de détails sur toutes les options de configuration de Sophos Control Center, qui ne sont pas abordées dans ce guide, consultez l'Aide de Sophos Control Center.

La documentation Sophos est disponible sur <http://www.sophos.fr/support/docs/>.

## 2 Configuration requise

Pour plus d'informations sur la configuration requise, consultez la page Configuration requise sur le site Web de Sophos <http://www.sophos.fr/products/all-sysreqs.html>.

Par ailleurs, vous devez disposer d'un accès Internet pour télécharger le logiciel depuis le site Web de Sophos.

Le Sophos Control Center et les autres composants serveur ont les autres conditions requises suivantes :

- Vous devez avoir accès aux autres ordinateurs du réseau et depuis ces derniers.
- Il est conseillé d'utiliser un système d'exploitation de type serveur (comme Windows Server 2003 ou Windows Small Business Server 2011). Autrement, les performances du Sophos Control Center seront affectées.

**Important :** si vous installez le Sophos Control Center sur Windows 2008 Small Business Server (SBS), assurez-vous que Windows Live OneCare n'est pas installé sur l'ordinateur. Pour désinstaller Windows Live OneCare, utilisez l'utilitaire Ajout/Suppression de programmes dans le Panneau de configuration Windows.

Si vous voulez utiliser SQL Server plutôt que SQL Server 2005 Express, qui est utilisé par Sophos pour ses produits, assurez-vous qu'il est installé et créez une instance "SOPHOS". Pour plus d'aide sur la manière de procéder, consultez votre documentation SQL Server ou le support technique de Microsoft.

## 3 Installation

### 3.1 Préparation de l'installation du Sophos Control Center

Avant d'installer le Sophos Control Center, assurez-vous :

- D'être en possession du nom utilisateur et du mot de passe fournis par Sophos.
- D'ouvrir une session en tant qu'administrateur ou en tant qu'administrateur de domaine, selon votre choix, sur l'ordinateur sur lequel vous voulez installer le Sophos Control Center.

**Remarque :** pour assurer la protection des ordinateurs qui sont dans un groupe de travail, quelle que soit la plate-forme Windows, effectuez d'abord les étapes supplémentaires décrites dans l'article : <http://www.sophos.fr/support/knowledgebase/article/29728.html>.

### 3.2 Préparation des ordinateurs

Avant d'installer le logiciel de sécurité sur vos ordinateurs, assurez-vous que :

- Le logiciel antivirus d'une autre éditeur est supprimé de tous les ordinateurs sur lesquels vous souhaitez installer Sophos Anti-Virus.
- Le système d'exploitation est configuré de manière appropriée.

#### 3.2.1 Windows Vista et supérieur

Sophos Anti-Virus nécessite la configuration supplémentaire suivante sur les ordinateurs Windows Vista et supérieur :

- Assurez-vous que le service **Registre à distance** est démarré et que son type de démarrage est défini sur **Automatique**. Ce service n'est pas activé par défaut sur Windows Vista. Accédez-y via **Démarrer|Panneau de configuration|Outils d'administration|Services**. Dans la liste déroulante des services, cliquez deux fois sur le service **Registre à distance**. Dans la boîte de dialogue **Propriétés de Registre à distance**, sur l'onglet **Général**, dans le champ **Type de démarrage**, cliquez sur la flèche du menu déroulant et sélectionnez **Automatique**. Cliquez sur **Appliquer**. Cliquez sur **Démarrer** et cliquez sur **OK**.
- Désactivez le **Contrôle des comptes d'utilisateurs**. Accédez-y via **Démarrer|Panneau de configuration|Comptes d'utilisateurs|Activer ou désactiver le contrôle des comptes d'utilisateurs**. A la fin de l'installation, activez de nouveau cette option.
- Ouvrez le **Pare-feu Windows avec fonctions avancées de sécurité**. Accédez-y via **Démarrer|Panneau de configuration|Outils d'administration**. Changez les **Règles de trafic entrant** pour activer les éléments suivants :

Nom de la règle	Profil
Administration à distance (NP-Entrée)	Domaine
Administration à distance (NP-Entrée)	Privé

Nom de la règle	Profil
Administration à distance (RPC)	Domaine
Administration à distance (RPC)	Privé
Administration à distance (RPC-EPMAP)	Domaine
Administration à distance (RPC-EPMAP)	Privé

**Remarque :** une fois l'installation terminée, désactivez de nouveau ces processus.

### 3.2.2 Windows XP

Effectuez les étapes suivantes sur tout ordinateur Windows XP disposant ou non d'un Service Pack :

- Supprimez tout autre logiciel de pare-feu, à l'exception du pare-feu Windows, de tous les ordinateurs Windows XP sur lesquels vous voulez installer Sophos Client Firewall.
- Désactivez le Partage de fichiers simple.

Pour savoir comment procéder, consultez l'article  
<http://www.sophos.fr/support/knowledgebase/article/12837.html>.

#### Windows XP avec Service Pack 2

Sur un ordinateur Windows XP avec Service Pack 2 dont le pare-feu Windows est activé et sur lequel vous **n'avez pas** l'intention d'installer Sophos Client Firewall, procédez de la manière suivante :

- Activez le Partage de fichiers et d'imprimantes pour les réseaux Microsoft.
- Ajoutez l'exception suivante du programme :

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

Pour savoir comment procéder, consultez l'article  
<http://www.sophos.fr/support/knowledgebase/article/11075.html>.

### 3.2.3 Windows Server 2003 avec Service Pack 1

Si le pare-feu Windows est activé, procédez de la manière suivante :

- Activez le Partage de fichiers et d'imprimantes pour les réseaux Microsoft.
- Ajoutez l'exception suivante du programme :

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

Pour savoir comment procéder, consultez l'article  
<http://www.sophos.fr/support/knowledgebase/article/11075.html>.

### 3.2.4 Windows 2000

- Supprimez tout autre logiciel de pare-feu, à l'exception du pare-feu Windows, de tous les ordinateurs Windows 2000 sur lesquels vous voulez installer Sophos Client Firewall.

### 3.2.5 Windows 98 SE

- Supprimez toute installation existante de Sophos Anti-Virus. Utilisez l'utilitaire Ajout/Suppression de programmes accessible via le Panneau de configuration Windows pour effectuer cette opération.

## 3.3 Installation du Sophos Control Center

Commencez par installer le Sophos Control Center qui vous permettra de télécharger, déployer et gérer les logiciels antivirus et de pare-feu.

1. Rendez-vous sur la page de téléchargement des produits Sophos sur <http://www.sophos.fr/support/updates> et saisissez le nom utilisateur et le mot de passe qui vous ont été fournis par Sophos.

Suivez les liens pour télécharger le programme d'installation de vos Solutions PME Sophos, puis exécutez-le.

2. Dans l'outil d'extraction (**programme d'installation de Sophos Small Business Edition**) confirmez le chemin d'extraction des fichiers d'installation (il doit impérativement se trouver sur le même ordinateur que celui sur lequel vous installez le Sophos Control Center) puis cliquez sur **Installer**.
3. Sur la page **Bienvenue**, cliquez sur **Suivant**.

Un assistant vous guide tout au long de l'installation. Acceptez les options par défaut, à l'exception de celles ci-dessous.

4. Sur la page **Type d'installation**, sélectionnez **Complète** pour installer toutes les fonctions du programme.

**Remarque :** si vous souhaitez administrer le logiciel de sécurité depuis un autre ordinateur, copiez le programme d'installation sur cet ordinateur, lancez-le et sélectionnez **Console d'administration seulement**.

Cliquez sur **Suivant** et poursuivez les étapes de l'assistant en conservant les options par défaut.

5. Une fois l'installation terminée, cliquez sur **Terminer** pour fermer la session automatiquement. Si vous voulez fermer la session ultérieurement, désélectionnez la case à cocher **Fermer la session maintenant** avant de cliquer sur **Terminer**.

Parfois, il est nécessaire de redémarrer Windows au lieu de simplement fermer la session. Dans ce cas, la case à cocher n'apparaît pas et un message vous demande si vous voulez redémarrer Windows maintenant ou ultérieurement.

6. Lorsque vous rouvrez une session, ouvrez-la avec le même nom d'utilisateur. L'Assistant Sophos de protection du réseau démarre automatiquement.

Pour plus d'informations sur la protection des ordinateurs en réseau, reportez-vous à la section [Protection des ordinateurs en réseau](#) à la page 9.

## 4 Protection des ordinateurs en réseau

Lorsque vous ouvrez une session pour la première fois suite à l'installation du Sophos Control Center, celui-ci s'ouvre automatiquement et l'Assistant Sophos de protection du réseau démarre. Cet assistant vous permet de protéger les ordinateurs en réseau.

1. Sur la page **Bienvenue**, cliquez sur **Suivant**.
2. Sur la page **Détails du compte de téléchargement Sophos**, saisissez le nom utilisateur et le mot de passe qui vous ont été fournis par Sophos et cliquez sur **Suivant**.

Sophos Control Center télécharge le logiciel dans un dossier sur l'ordinateur que vous êtes actuellement en train d'utiliser et le distribue depuis cet emplacement sur d'autres ordinateurs. L'emplacement diffère selon le système d'exploitation :

- Windows 2000, XP et 2003 :  
C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista et supérieur :  
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

Si vous utilisez un serveur proxy pour vous connecter à Internet, sélectionnez **Accéder à Sophos via un serveur proxy** et saisissez les détails du proxy.

3. Sur la page **Sélection des plate-formes**, sélectionnez le logiciel pour les systèmes d'exploitation s'exécutant sur votre ordinateur.
  - L'option **Windows 2000 et supérieur** est sélectionnée par défaut.
  - Si vous disposez d'ordinateurs Mac OS X, sélectionnez la case Mac OS X. Ainsi, vous pourrez ultérieurement installer le logiciel antivirus sur les ordinateurs.
4. Sur la page **Téléchargement des logiciels**, une barre de progression apparaît. Le Sophos Control Center télécharge le logiciel. Lorsque le téléchargement est terminé, cliquez sur **Suivant**.
5. Sur la page **Détails du compte utilisateur Windows**, saisissez les détails d'un compte ayant les droits administrateur, qui est valide sur tous les ordinateurs en réseau et qui peut être utilisé pour installer le logiciel sur ces ordinateurs. Il ne s'agit pas du même compte que le compte Sophos utilisé plus haut. Dans la plupart des cas, vous pouvez utiliser le compte avec lequel vous avez ouvert une session avant de commencer l'installation.
6. Sur la page **Protection des ordinateurs**, l'assistant recherche les ordinateurs sur lesquels le logiciel peut être installé automatiquement.

Seuls les ordinateurs Windows 2000 et supérieur apparaissent sur cette page, en effet, l'installation automatique n'est pas possible sur les ordinateurs Windows 98 ou sur les ordinateurs Mac.

Par défaut, tous les ordinateurs sont sélectionnés pour recevoir la protection. Vous pouvez dessélectionner la case de tout ordinateur pour lequel vous ne souhaitez pas appliquer la protection. Pour sélectionner ou dessélectionner toutes les cases à cocher de la liste, sélectionnez ou dessélectionnez la case à cocher se trouvant dans l'en-tête de la colonne **Protection**.

7. Sur la page **Sélection des fonctionnalités**, sélectionnez les fonctionnalités que vous désirez installer :

- Protection antivirus (sélectionnée par défaut).
- Protection Sophos Client Firewall (s'il est inclut dans votre licence).

**Remarque :** redémarrez chaque ordinateur sur lequel vous avez choisi d'installer Sophos Client Firewall pour activer le pare-feu.

- Outil de suppression du logiciel concurrent.

Cliquez sur **Suivant**.

8. Si des ordinateurs apparaissent dans la page **Ordinateurs que vous devez protéger manuellement**, cliquez sur **Imprimer** pour imprimer la liste de ces ordinateurs, cliquez sur **Enregistrer sous** pour enregistrer une copie de la liste, ou prenez-en note. Cliquez sur **Suivant** et suivez les instructions de l'assistant.

Le Sophos Control Center installe le logiciel automatiquement sur les ordinateurs que vous avez sélectionné.

Au moment où la protection antivirus et de pare-feu est appliquée à chaque ordinateur, une icône bleue d'ordinateur près du nom de l'ordinateur apparaît et la colonne **A jour** affiche le mot **Oui**.

Pour plus d'informations sur la protection manuelle des ordinateurs, reportez-vous à la section [Protection manuelle des ordinateurs en réseau](#) à la page 10.

## 4.1 Protection manuelle des ordinateurs en réseau

Vous pouvez protéger les ordinateurs manuellement.

1. Rendez-vous sur chaque ordinateur de la liste que vous avez imprimée ou enregistrée. Naviguez jusqu'au dossier depuis lequel le Sophos Control Center met les logiciels antivirus et de pare-feu à disposition. Par défaut, les dossiers sont les suivants :

Système d'exploitation	Dossier
Windows 2000 et supérieur	\\[nom serveur]\sophosUpdate\CIDs\Sxxx\EECSXP
Windows 98	\\[nom serveur]\sophosUpdate\CIDs\Sxxx\ES9X
Mac OS X	smb://[nom serveur]/sophosUpdate/CIDs/Sxxx/ESCOSX

où :

[nom serveur] correspond au nom de l'ordinateur sur lequel vous avez installé le Sophos Control Center.

[Sxxx] correspond au nombre généré au cours du téléchargement, par exemple, S000.

2. Cliquez deux fois sur setup.exe (sous Windows) ou sur Sophos Anti-Virus.mpkg (sous Mac OS X).

Si vous effectuez l'installation sur Mac OS X 10.2 ou supérieur, copiez Sophos Anti-Virus.mpkg sur le Mac, et effectuez l'installation depuis cet ordinateur.

À présent, vous pouvez également protéger les ordinateurs qui ne sont pas toujours connectés au réseau ([Protection des ordinateurs occasionnellement connectés à votre réseau](#) à la page 11).

## 4.2 Protection des ordinateurs occasionnellement connectés à votre réseau

Les ordinateurs qui sont occasionnellement connectés à votre réseau (par exemple, les ordinateurs portables qui sont utilisés à l'extérieur du bureau, mais qui y sont aussi amenés) peuvent être protégés même s'ils ne sont pas sur le réseau.

Tous les ordinateurs sur lesquels vous avez installé les logiciels antivirus et de pare-feu sont déjà configurés pour récupérer leurs mises à jour antivirus et de pare-feu directement depuis Sophos lorsqu'ils ne sont pas connectés à votre réseau.

S'il y a des ordinateurs qui sont occasionnellement connectés à votre réseau, sur lesquels vous n'avez pas encore installé les logiciels antivirus ou de pare-feu, protégez-les lors de leur prochaine connexion à votre réseau. Cette opération est expliquée dans l'Aide du Sophos Control Center à la section sur la protection des nouveaux ordinateurs.

## 5 Vérification de la protection des ordinateurs

Vous pouvez vérifier que vos ordinateurs en réseau sont protégés contre les menaces grâce au Tableau de bord.

Le Tableau de bord vous donne une visibilité immédiate de l'état de sécurité du réseau. Vous pouvez configurer les valeurs seuil de déclenchement d'avertissements et d'envoi de messages d'alerte par le Tableau de bord lorsqu'une valeur seuil est atteinte.

Pour afficher ou masquer le Tableau de bord, cliquez sur le bouton **Tableau de bord** de la barre d'outils.

Pour plus d'informations sur la configuration du Tableau de bord et une liste complète des icônes qui apparaissent ainsi que leur état, reportez-vous à l'Aide du Sophos Control Center.

## 6 Paramétrage des alertes par courriel

Par défaut, les alertes de bureau apparaissent seulement sur l'ordinateur sur lequel la menace est trouvée. Vous pouvez configurer le Sophos Control Center afin que vos utilisateurs reçoivent également une alerte par courriel lors de la découverte d'une menace.

Pour configurer les alertes par courriel pour les menaces :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Messagerie**.

La boîte de dialogue **Messagerie** apparaît.

3. Cliquez sur l'onglet **Alertes par courriel**, sélectionnez **Activer les alertes par courriel** pour recevoir les alertes par courriel.
4. Dans le volet **Messages à envoyer**, sélectionnez les événements pour lesquels vous voulez envoyer des alertes par courriel.

**Remarque :** les paramètres Détection des comportements suspects, Détection des fichiers suspects et Détection et nettoyage des adwares et des PUA s'appliquent seulement à Windows 2000 et supérieur. Le paramètre Autres erreurs s'applique uniquement à Windows.

5. Dans le volet **Destinataires**, cliquez sur **Ajouter** ou sur **Supprimer** pour respectivement ajouter ou supprimer des adresses électroniques auxquelles les alertes par courriel doivent être envoyées. Cliquez sur **Renommer** pour changer une adresse électronique que vous avez ajoutée.

**Remarque :** les ordinateurs Mac OS X envoient uniquement des messages au premier destinataire de la liste.

6. Cliquez sur **Configurer SMTP** pour changer les paramètres du serveur SMTP et la langue des alertes par courriel
7. Dans la boîte de dialogue **Configuration des paramètres SMTP**, saisissez les détails comme décrit ci-dessous :

- Dans la zone de texte **Serveur SMTP**, saisissez le nom d'hôte ou l'adresse IP du serveur SMTP. Cliquez sur **Tester** pour vérifier si l'envoi de l'alerte par courriel fonctionne.
- Dans la zone de texte **Adresse expéditeur SMTP**, saisissez une adresse électronique à laquelle les messages renvoyés et les rapports de non-distribution peuvent être envoyés.
- Dans la zone de texte **Adresse réponse SMTP**, vous pouvez saisir une adresse électronique à laquelle les réponses aux alertes par courriel peuvent être envoyées. Les alertes par courriel sont envoyées depuis une boîte aux lettres sans surveillance.

**Remarque :** les ordinateurs Linux et UNIX ignorent les adresses expéditeur et réponse SMTP et utilisent l'adresse `root@<nomhôte>`.

- Dans le volet **Langue**, cliquez sur la flèche du menu déroulant et sélectionnez la langue dans laquelle les alertes par courriel doivent être envoyées.

Vous pouvez également configurer le Sophos Control Center pour envoyer des alertes par courriel à propos de l'état du réseau en fonction des seuils atteints sur le Tableau de bord. Pour

plus d'informations, reportez-vous à la section Gestion des notifications dans l'Aide du Sophos Control Center.

## 7 Paramétrage de la recherche des applications potentiellement indésirables

Par défaut, Sophos Anti-Virus détecte les virus, les chevaux de Troie, les spywares et les vers. Vous pouvez aussi configurer le logiciel pour qu'il détecte les applications potentiellement indésirables (PUA).

**Remarque :** cette option s'applique uniquement à Sophos Anti-Virus pour Windows 2000 ou supérieur.

Sophos vous conseille de commencer par utiliser un contrôle planifié pour détecter les applications potentiellement indésirables. Ainsi, vous pouvez gérer en toute sécurité les applications qui sont déjà en cours d'exécution sur votre réseau. Vous pouvez ensuite activer le contrôle sur accès des applications potentiellement indésirables pour protéger vos ordinateurs à l'avenir.

### 7.1 Exécution d'un contrôle planifié sur les ordinateurs

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, dans le volet **Contrôle planifié**, cliquez sur **Ajouter** pour créer un nouveau contrôle ou sélectionnez un contrôle dans la liste et cliquez sur **Modifier** pour le modifier.
3. Dans la boîte de dialogue **Contrôle planifié**, cliquez sur **Configurer** (en bas de la page).
4. Dans la boîte de dialogue **Paramètres de contrôle et de nettoyage**, cliquez sur l'onglet **Contrôle**. Dans le volet **Autres options de contrôle**, sélectionnez la case **Rechercher les adwares et les PUA** et cliquez sur **OK**.

Lorsque le contrôle s'effectue, Sophos Anti-Virus peut signaler certaines applications potentiellement indésirables. Vous pouvez soit autoriser les applications soit les supprimer des ordinateurs.

### 7.2 Autorisation des applications que vous voulez utiliser

Vous pouvez choisir d'autoriser les applications qui ont été détectées en tant qu'adware/PUA au cours d'un contrôle planifié.

Pour autoriser une application :

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.
2. Dans la boîte de dialogue **Configuration du contrôle**, cliquez sur **Autorisation**.
3. Dans la boîte de dialogue **Gestionnaire d'autorisation**, procédez ainsi :
  - Sélectionnez l'application que vous voulez autoriser. Cliquez sur **Ajouter** pour l'ajouter à la liste des applications autorisées.
  - Si vous ne pouvez pas voir l'application, cliquez sur **Nouvelle entrée**. Dans la boîte de dialogue qui s'ouvre, suivez le lien vers la liste Sophos des applications potentiellement indésirables. Recherchez l'application que vous voulez autoriser et saisissez son nom dans le champ **Nom**.

## 7.3 Nettoyage des applications que vous ne voulez pas utiliser

Vous pouvez nettoyer les applications qui ont été détectées en tant qu'adware/PUA au cours d'un contrôle planifié.

Pour nettoyer les applications :

1. Dans le volet gauche, sous **Action**, cliquez sur **Résolution des alertes et des erreurs**.

La boîte de dialogue **Résolution des alertes et des erreurs** apparaît.

2. Sélectionnez la case à cocher pour chaque application que vous souhaitez supprimer ou cliquez sur **Tout sélectionner**, puis cliquez sur **Nettoyer**.

Cette opération supprime tous les composants connus des applications sélectionnées des ordinateurs sélectionnés. L'opération de nettoyage peut prendre quelques minutes.

**Remarque :** il existe certaines applications que vous ne pouvez pas nettoyer à l'aide du Sophos Control Center. Dans ce cas, allez sur l'ordinateur affecté et nettoyez l'application à l'aide de Sophos Anti-Virus.

Pour nettoyer complètement un ordinateur de certaines applications à plusieurs composants, il se peut que vous ayez à redémarrer l'ordinateur. Si c'est le cas, un message apparaîtra sur l'ordinateur affecté, vous donnant le choix de redémarrer l'ordinateur immédiatement ou ultérieurement. Les étapes finales de nettoyage sont effectuées après le redémarrage de l'ordinateur.

Pour en savoir plus sur une application donnée sur le site Web de Sophos, dans la boîte de dialogue **Résolution des alertes et des erreurs**, cliquez sur le nom de l'application.

Si vous cliquez sur **Approuver**, les applications sélectionnées sont supprimées de la liste. Par contre, elles ne sont ni nettoyées ni autorisées.

## 7.4 Activation du contrôle sur accès pour les adwares et les applications potentiellement indésirables

1. Dans le volet gauche, sous **Configuration**, cliquez sur **Configurer le contrôle**.

La boîte de dialogue **Configuration du contrôle** apparaît.

2. Cliquez sur **Contrôle sur accès**.

La boîte de dialogue des **Paramètres du contrôle sur accès** apparaît.

3. Dans le volet **Options de contrôle**, sélectionnez la case **Rechercher les adwares et les PUA**. Cliquez sur **OK**.

Certaines applications "surveillent" les fichiers et tentent d'y accéder régulièrement. Si le contrôle sur accès est activé, il détecte chaque accès et envoie plusieurs alertes.

## 8 Traitement des virus

Vous pouvez nettoyer les virus en procédant de la manière suivante :

1. Dans le Sophos Control Center, sur le **Tableau de bord**, cliquez sur le lien **Virus/spywares**.

Dans la boîte de dialogue **Résolution des alertes et des erreurs**, une liste d'ordinateurs infectés, accompagnée des détails sur les virus, apparaît.

2. Sélectionnez les virus que vous voulez nettoyer et cliquez sur **Nettoyer**.

Cette opération supprime le virus du fichier ou du secteur de démarrage qui a été infecté. Toutefois, le nettoyage des documents ne répare pas les modifications que le virus a apportées au document et le nettoyage des programmes doit uniquement être utilisé en tant que mesure temporaire : remplacez ensuite les programmes nettoyés depuis les disques originaux ou depuis une sauvegarde saine. L'opération de nettoyage peut prendre quelques minutes.

Certains virus ne peuvent pas être nettoyés à l'aide du Sophos Control Center. Dans ce cas, allez sur l'ordinateur affecté et nettoyez le virus à l'aide de Sophos Anti-Virus

Avant de tenter de nettoyer des menaces à plusieurs composants des ordinateurs, Sophos vous conseille d'exécuter un contrôle à la demande complet des ordinateurs afin de déterminer tous les composants des menaces à plusieurs composants.

Pour en savoir plus sur un virus particulier sur le site Web de Sophos, dans la boîte de dialogue **Résolution des alertes et des erreurs**, cliquez sur le nom du virus.

## 9 Configuration du pare-feu

Lorsque vous installez Sophos Client Firewall pour la première fois, celui-ci est configuré pour autoriser le trafic entrant essentiel et le trafic sortant.

**Remarque :** Sophos Client Firewall ne prend pas en charge IPv6. La version 1 laisse passer les paquets IPv6 alors que les versions 1.5 et 2.0 bloquent tous les paquets IPv6 ou les autorisent tous selon la configuration.

### 9.1 Configuration du pare-feu

Vous pouvez configurer le pare-feu pour autoriser ou bloquer le trafic selon votre choix. Par défaut, le pare-feu est paramétré pour autoriser le trafic entrant essentiel et tout le trafic sortant.

Pour configurer le pare-feu :

1. Dans le volet de gauche, sous **Configuration**, cliquez sur **Configurer le pare-feu**.
2. Sur l'Assistant de configuration du pare-feu, cliquez sur **Suivant**.
3. Sur la page **Configuration du pare-feu**, sélectionnez l'une des options suivantes :
  - **Emplacement unique**  
Sélectionnez cette option pour les ordinateurs qui sont toujours connectés à votre réseau, par exemple, les ordinateurs de bureau.
  - **Emplacement double**  
Sélectionnez cette option si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau (sur le réseau) et en dehors du bureau. Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.
  - **Autoriser tout le trafic**  
Sélectionnez cette option si vous voulez désactiver le pare-feu et autoriser tout le trafic.
4. Si vous avez sélectionné **Emplacement double** sur la page précédente, sur la page **Identification réseau**, configurez l'identification DNS ou passerelle de votre réseau.

**Remarque :** la page **Identification réseau** apparaît seulement si vous sélectionnez **Emplacement double**.

Le Sophos Control Center applique ensuite les différents paramètres du pare-feu sur les ordinateurs en fonction de leur emplacement, c'est-à-dire sur le réseau ou en dehors du réseau.

5. Sur la page **Mode de fonctionnement**, sélectionnez un mode selon lequel le pare-feu doit gérer le trafic entrant et sortant.
  - **Bloquer le trafic entrant et autoriser le trafic sortant**

Autorise uniquement le trafic entrant essentiel à accéder au réseau et à Internet et bloque tout le trafic entrant. Les applications ne sont pas authentifiées dans ce mode.
  - **Bloquer le trafic entrant et sortant**

Si vous sélectionnez ce mode, le pare-feu va bloquer tout le trafic sortant, à l'exception des applications que vous avez spécifiées. Cliquez sur le bouton **Accepter** à la droite de cette option pour ajouter des applications. Pour une application "acceptée", toute l'activité du réseau est autorisée.
  - **Surveiller**

Ce mode applique toutes les règles que vous avez définies sur vos ordinateurs et autorise également tout le trafic inconnu à accéder au réseau et à Internet. Sous ce mode, les informations sont envoyées à la console. Utilisez ce mode pour collecter des informations sur votre réseau et créer des règles appropriées.
  - **Personnaliser**

Vous permet d'appliquer une configuration personnalisée. Cliquez sur **Avancés** pour ouvrir une configuration avancée pour le pare-feu.

**Remarque :** il s'agit d'une option avancée que vous devez utiliser uniquement si vous connaissez les effets des changements que vous apportez.

Pour plus d'informations sur la configuration avancée du pare-feu, reportez-vous à *l'Aide de Sophos Endpoint Security and Control*.
6. Sur la page **Partage de fichiers et d'imprimantes**, sélectionnez **Autoriser le partage de fichiers et d'imprimantes** si vous souhaitez permettre aux autres ordinateurs de votre réseau local d'accéder aux imprimantes et aux dossiers partagés de votre ordinateur.
7. Si vous avez sélectionné **Emplacement double**, vous allez être invité à choisir un mode de fonctionnement et au partage de fichiers et d'imprimantes (mentionné aux étapes 5 et 6) pour l'emplacement secondaire (hors réseau).

Vous pouvez choisir d'exécuter de nouveau l'assistant, si vous choisissez de modifier ultérieurement l'un des paramètres.

Après avoir paramétré le pare-feu, vous pouvez consulter les événements de pare-feu (par exemple, les applications bloquées par le pare-feu) dans **Pare-feu - Observateur d'événements**. Pour plus d'informations, reportez-vous à l'Aide du Sophos Control Center.

## 9.2 Traitement des éléments bloqués par le pare-feu

Sophos Control Center peut bloquer les applications ou les processus que vous décidez de vouloir exécuter. Si c'est le cas, procédez de la manière suivante :

1. Dans le Sophos Control Center, sur le **Tableau de bord**, cliquez sur le lien **Pare-feu**.
2. Dans la boîte de dialogue **Pare-feu - Observateur d'événements**, sélectionnez l'entrée de l'application pour laquelle vous voulez autoriser ou créer une règle. Cliquez sur **Créer une règle**.

3. Dans la boîte de dialogue qui apparaît, indiquez si vous voulez autoriser l'application ou lui créer une règle à l'aide d'une option prédéfinie existante.

## 10 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à [support@sophos.fr](mailto:support@sophos.fr), y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

## 11 Copyright

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

Les logiciels Sophos mentionnés dans le présent document incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à [support@sophos.fr](mailto:support@sophos.fr) ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>

18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

**iMatix SFL**

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation  
<<http://www.imatix.com>>.